November 2018

MOD POLICY ON THE PASSING OR RECEIPT OF INTELLIGENCE RELATING TO DETAINED OR CAPTURED PERSONS

Context

1. Intelligence and information sharing is an important enabler for a range of UK defence activity, and is practised by a number of military and civilian organisations across MOD. However, it is vital that all UK military and MOD personnel involved in intelligence sharing understand that certain procedures must be applied when supplying or receiving intelligence in connection with detainees or detention operations (see the criteria in para 13 below). For the purposes of this policy, the UK receiver or supplier of the intelligence is referred to as the "official" and may be military or civilian.

2. It is HMG policy that UK personnel should not participate in, condone, solicit or encourage torture or cruel, inhuman or degrading treatment or punishment (CIDT). Thus when supplying or receiving intelligence about, or derived from, someone detained (or whom we believe is likely to be detained) by another nation, officials must consider carefully whether that person has been subjected to torture, CIDT or another form of unacceptable treatment (as defined in Annex A), or is at risk of being subjected to such treatment.

3. This policy is set out in the Cabinet Office Consolidated Guidance (CG), published in July 2010[1], which, among other things, states that if there is a 'serious risk' of torture the presumption is that intelligence should not be shared. If there is a 'serious risk' of torture or CIDT, Ministerial authorisation should be sought. This MOD policy note amplifies the CG, by setting out what steps must be taken (including record-keeping in the format at Annex B) by MOD officials when considering the supply or receipt of intelligence relating to a potential detainee or derived from a current detainee held by a third party. This need not necessarily mean that an individual is named in the intelligence, but that a particular individual could be detained or an existing detainee put at risk of torture or CIDT on the basis of the intelligence shared (possibly when combined with information the third party already holds).

4. The criteria for engaging the CG are set out at para 13. If the intelligence does not meet these criteria then CG is not engaged, and normal intelligence sharing arrangements apply. The CG should not therefore impact on the routine, working level sharing of battlefield information and observations, which is a key part of working alongside local security forces on many UK operations. For example, CG does not apply where a UK sentry observes insurgent activity in the vicinity of local security forces, and informs these forces of what he/she has seen or heard in in order for them to interdict the threat and take appropriate defensive action.

5. Theatre-specific instructions for deployed operations will be issued by the relevant operational headquarters[2] where necessary. Further advice on the assessment of risks of

---

[1] HM Government Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees, July 2010. Note that a detainee may be someone military or civilian captured in an operational theatre (CPERS), otherwise detained by the host nation, or held subject to judicial proceedings in that nation.

[2] For example, PJHQ.

torture or CIDT by the local or coalition detention authority involved can be sought from senior personnel[3] or from the contact points listed at the end of this policy.

Principles

6. The purpose of the procedures set out below is to assess the risk of torture or CIDT to the person to whom the intelligence relates or from whom it is derived and to enable decision making at the appropriate level. Where there is a serious risk of torture which cannot be effectively mitigated, there is a presumption that intelligence will not be shared. If an official believes there is a serious risk of torture or CIDT, including after any mitigating measures, then approval to supply or receive the intelligence must be sought from Ministers. The guiding principle is that this risk requires a very careful analysis and explanation, as do the risk mitigations and the assessment of their likely effectiveness. The anticipated benefits of intelligence sharing should also be clearly articulated.

Risk Assessment

7. The official is responsible for the initial risk assessment and either proceeding with the intelligence sharing or referring up to senior personnel for further risk assessment, including legal advice if appropriate. These risk assessments will take into consideration two aspects:

- **An organisational assessment.** This will consider the facilities within which the detainee may be held and the organisation and individuals involved in running the facilities. The assessment will consider the risk that individuals detained by that organisation or within that facility will be subject to torture or CIDT, as well as consider its legal framework and wider practices. As far as possible, these assessments will reflect the views of other government departments and agencies.

- **A detainee assessment.** The detainee assessment will consider whether the particular detainee(s) or potential detainee(s) in question would be put at serious risk by the proposed action. It should assess whether there is any reason to believe that the risk of torture or CIDT for the particular detainee(s) is likely to be different from that identified in the organisational assessment.

8. During enduring operations in which there is likely to be a frequent requirement to share intelligence that invokes the CG, the relevant operational headquarters, in consultation with SPO, may decide to issue standing organisational assessments for the main facilities or organisations involved. Completion of the standing organisational assessment is the responsibility of the operational headquarters, but these should also be passed to SPO. For the avoidance of doubt, these assessments will be applicable to all officials in theatre, not just those under the command of the operational headquarters that completed the assessment. Assessments should be formally reviewed at six-month intervals or whenever significant new information comes to light that may alter the assessment.

9. There will inevitably be a degree of judgement in deciding whether the risk is serious, and how effective any mitigation might be. Personnel involved in intelligence sharing

[3] The appropriate senior personnel within the official's command chain will be identified by the operational headquarters or Defence Intelligence (DI).

should take reasonable steps to familiarise themselves with the treatment of detainees by the third party involved using all the information at their disposal, including:

- any standing organisational risk assessments covered in para 8;
- any additional risk assessments of the detaining authorities (including intelligence reporting and reports produced by NGOs and Human Rights Bodies);
- the official's own experience.

10. If there is any evidence of torture or CIDT but it is deemed to be isolated, or can be explained by reference to factors that do not apply to the current case, it might be considered that any risk is "lower than serious". However, any reference to widespread or systemic torture or CIDT, or even instances which are rare but there is reason to believe they may re-occur, could lead to the assessment of risk being "serious". Where the information available is not sufficient to support a reasonable assessment of risk, it may be necessary to err on the side of caution and escalate to senior personnel, as described in the procedures below.

Risk Mitigation

11. Mitigations might include seeking reliable assurances from the detaining authority over the treatment of the person, or establishing an independent oversight of the detention facility or the detainee. In practice, some mitigations, especially assurances, will have been or will need to be sanctioned by a higher authority, and the official should always inform the operational headquarters or DI (by passing on the partially completed form) of the mitigations taken or sought. Operational headquarters, in association with SPO, may issue guidance on what mitigating measures are appropriate for specific facilities or organisations.

12. Where the risk of torture or CIDT is assessed as serious, mitigation measures should be identified that might reduce the level of risk. A reasonable assessment should be made of the likely effectiveness of such measures and this should form part of the overall judgement on whether Ministers should be consulted (i.e. whether the residual risk remains serious). Where the assessment is that there is a serious risk of torture, clearly there would need to be high confidence in the effectiveness of the mitigation to support lowering the risk assessment.

Procedures

13. The first step in determining whether CG is engaged is for the civilian or military official to decide whether the intelligence in question:

- is about a detainee (including captured personnel (CPERS)) held by a third party; or
- has been obtained from a detainee held by a third party; or
- will be put to a detainee held by a third party (including passing questions to be put to a detainee, or directly participating in interviews under a third party's control); or
- is likely to be used by a third party to detain a particular person or persons (either at the third party's own initiative or at UK request);

14. If any of the above apply, CG is engaged and the risk of torture or CIDT to the person must be assessed, and the processes outlined below must be followed before proceeding.

Where there is any uncertainty over whether a criterion is met, advice must be sought from senior personnel before proceeding. Whether or not advice is sought, records must be kept in the form set out at Annex B.

15. As soon as it has been determined that one or more of the criteria above are met, the official must take the following steps.

i. Summary. The official begins completion of the form at Annex B, in accordance with the guidance in this policy, by setting out the details of the intelligence and the detainee (or prospective detainee) involved and selecting the criteria engaged (see para 13).

ii. Assessment of Risk. The official assesses the risk of torture or CIDT of the detainee or prospective detainee. This assessment will include circumstances particular to the intelligence or to the detainee involved, as well as more generic assessments of the risks associated with the detaining party (see para 7). In some cases, standing organisational assessments will be held and will be available to the official via their operational headquarters (see para 8). Those consulted for advice, and the advice given, must be recorded using the form at Annex B.

iii. It is vital that the official sets out clearly the factors that have informed their assessment and that they identify any areas where they do not have all the relevant information about an individual, organisation or likely outcome (see paras 9 and 10). In all cases they should set out:

- what we know and any key areas where information is lacking (including all sources of information on which the assessment is based);
- the assessed risk of torture or CIDT;
- if there are any concerns, what mitigating measures are available;
- the likely effectiveness of these mitigation measures and therefore whether the risk is reduced.

iv. Benefit. Where there is a risk of torture or CIDT, however serious, the official should set out what benefits are likely to accrue to the operation from sharing intelligence as proposed and how likely these benefits are to materialise.

v. Lower than serious risk. If an official concludes there is no risk of torture or CIDT, or the risk is considered to be lower than serious, they may proceed without further authority. The partially completed Annex B form must be retained for audit and oversight purposes (see para 23).

vi. Serious risk which can be mitigated at the official's level. If there is assessed to be a serious risk of torture or CIDT, but there are mitigations either already in place or available to the official to reduce the risk below that level in the case in question, then the official must identify these mitigations and confirm on the form that they have been carried out and have reduced the risk assessment to lower than serious before proceeding. The partially completed form and any correspondence relating to its contents must be retained for audit and oversight purposes (see para 23).

vii. Serious risk which can be mitigated by senior personnel. If the risk of torture or CIDT cannot be effectively mitigated at the official's level, the official must consult senior personnel, passing the form to them for additional comments and assessment.

The senior personnel must consider whether higher-level or alternative mitigation measures can be taken to reduce the risks. Where the senior personnel conclude the risk can be effectively mitigated below the serious risk threshold, the intelligence sharing can proceed.

viii. Serious risk of CIDT which cannot be mitigated. If the risk of CIDT remains serious post mitigation, or if there are perceived additional policy/legal or reputational risks, Ministers should be consulted through the operational headquarters or DI Sec. The Ministerial submission should clearly articulate the operational benefits of sharing the intelligence, the risk of CIDT, mitigations and their likely effectiveness, and, separately, the legal risk in terms of likelihood of legal challenge and, if challenged, the prospects of the challenge's success.

ix. Serious risk of torture which cannot be mitigated. Where there remains a serious risk of torture post mitigation, Ministers should be consulted as outlined above but the presumption would be that we will not proceed unless Ministers agree that the potential benefits justify accepting the risk and the legal consequences that may follow.

x. If it is known or believed that torture will take place, the official or senior personnel should raise concerns with the liaison or detaining authority to try to prevent the torture occurring, unless doing so might make the situation worse for the detainee. Ministers should be notified in this situation.

Special Cases

16. Urgent Approval. The CG recognises there may be situations – where UK Armed Forces personnel are operating under time sensitive military operational conditions – where personnel may need to share intelligence with coalition partners where there is no opportunity to seek guidance on any concerns over standards of detention or treatment, or refer to senior personnel or Ministers for approval. This may occur when:

- Suitably trained and qualified personnel are engaged in time-sensitive tactical questioning of detainees held by other nations;
- Intelligence reveals an imminent threat to life, which must be shared to avert the threat and save life; or
- UK forces have just been subject to attack and intelligence must be passed immediately to facilitate operations against those responsible, otherwise the opportunity to take action against the attackers would be lost.

17. If such situations arise, the decision should be approved at the highest level possible in the limited time available, and personnel should continue to observe this guidance so far as is practicable and report all the circumstances to their operational headquarters via their chain of command at the earliest opportunity. The Annex B form must be completed retrospectively (within 48 hours).

18. Unsolicited Intelligence. Where the third party does not disclose the sources of their intelligence it might not be apparent whether intelligence received has originated from a detainee or, if it has, to what standards that detainee may have been subject. However, in cases where officials receive unsolicited intelligence that they know or believe has originated from a detainee, an assessment of risk should be completed and recorded retrospectively on an Annex B. Where they have cause to believe that the standards to

which the detainee has been subject are unacceptable, or there is a serious risk of torture or CIDT, senior personnel must be informed. In all cases where senior personnel believe these concerns are valid, Ministers must be informed. In such instances, the senior personnel will consider whether action is required to ensure that continued receipt of intelligence is not seen to be encouraging the methods used to obtain it. Such action could, for example, include obtaining assurances, or demarches on intelligence and/or diplomatic channels. They will also consider whether the concerns were such that further engagement with the third party should cease.

19. Where biometric, photographic or other evidential information about a detainee in UK custody is to be passed to a third party for the express purpose of having them taking over custody of, and/or prosecuting, the individual, the risk assessment required by the CG should have already been made by the operational headquarters and MOD, and detainee transfers authorised in advance as a matter of policy. The form at Annex B is not required to be completed in these circumstances.

20. UK personnel frequently operate with trusted partners or third party authorities using shared intelligence databases. Where such a database exists, it has been assumed that an assessment has already been conducted by the UK participants on the standards and practices of those partners with access to such databases to conclude that there is no serious torture or CIDT risk associated with the pooling of this data. However, if in any doubt about who has access to such a database and the risk associated with such parties, officials should consult senior personnel and follow the processes in this paper.

21. CG aspects would need to be considered and recorded for any new intelligence databases set up as part of a future coalition or intelligence relationship. Existing assessments should also be revisited if any information comes to light to suggest that the level of risk has changed materially. However, CG is not engaged where forensically recovered biometric information which is not linked to a specific known individual (e.g. fingerprints taken from an IED which do not match an intelligence database of suspects) is loaded onto a database shared with trusted coalition partners or trusted third party authorities.

22. Pre-approval. In cases involving intelligence relating to an acknowledged high-threat individual, where all the information required to make a CG assessment is known apart from a key trigger (i.e. the location of the individual) and there is a serious risk of CIDT, it is possible to seek prior Ministerial approval for the intelligence to be shared. This would enable action to be taken swiftly if and when the final piece of intelligence becomes available. This procedure is to be used only in exceptional circumstances, against limited numbers of individuals at any one time, and reviewed on a regular basis (maximum two weeks). SPO, the relevant operational headquarters or DI should be consulted before this option is pursued.

Oversight and record keeping

23. The Intelligence Services Commissioner is responsible for monitoring implementation of CG, and looks to MOD SPO to provide full records of all events where the CG is assessed to be engaged. It is therefore important that records are made by officials and the operational headquarters on each occasion when this policy is engaged (including partially completed Annex B forms), and passed to the records contact point below for safe keeping, and onward transmission to SPO if requested. Ministerial submissions must be copied to SPO.

~~Contact points~~

Standing organisational assessments of the risks associated with the detention authorities in a specific operational theatre will be held by PJHQ, DI staff, or SPO. Refer to theatre-specific SOI or policy guidance for specific contact points.

For further advice on the CG or on MOD policy, refer to your theatre chain of command, LEGAD or POLAD; or DI staff, [redacted]

Completed and partially completed forms, and any Ministerial submissions, will be held by the relevant authority and will be made available to SPO on request.

ANNEX A:

DEFINITIONS OF UNACCEPTABLE STANDARDS OF TREATMENT OR DETENTION

1. For the purposes of this internal guidance, personnel should treat the following as unacceptable standards of treatment or detention. This Annex includes more terms than the Annex to the Cabinet Office Consolidated Guidance, but is still not exhaustive, nor is it descriptive of any legal term.

Unlawful arrest and detention

2. Officials should take account of:

a. The lawfulness of arrest (under local law).
b. The lawfulness of detention (under local and international law) and access to due process.

3. Considerations here may include:

- 'Incommunicado detention' (denial of access to family or legal representation, where this is incompatible with international law);
- Whether the detainee has been given the reasons for their arrest;
- Whether the detainee will be brought before a judge and when that will occur;
- Whether the detainee can challenge the lawfulness of their detention;
- The conditions of detention;
- Whether the detainee will receive a fair trial.

4. Legal advice should be sought when there are concerns about the lawfulness of detention under local and international law, particularly when dealing with states where the government is not recognised by the UK.

Torture

5. An offence under UK law, torture is defined as a public official intentionally inflicting severe mental or physical pain or suffering on an individual in the performance or purported performance of his official duties.

Cruel, inhuman or degrading treatment or punishment

6. CIDT is a term which is used in some international treaties but is not defined in UK law. In the context of this guidance, the UK Government considers that the following practices, *which is not an exhaustive list,* could constitute CIDT:

- Use of stress positions;
- Sleep deprivation;
- Methods of obscuring vision (except where these do not pose a risk to the detainee's physical or mental health and are necessary for security reasons during arrest or transit) and hooding;
- Physical abuse or physical/unlawful punishment of any sort;
- Withdrawal of food, water or medical help;
- Degrading treatment (sexual embarrassment, religious taunting etc);

- Deliberate use of 'white' or other noise.

7. In any case of doubt, personnel should seek guidance from senior personnel (or consult JDP 1 10) who may take appropriate advice on whether any conduct may amount to torture or CIDT.

Unlawful killing

8. The legal issues around the use of lethal force can be complex and will depend on a number of factors, not all of which may be known. Countries may differ in their interpretation of the relevant international law. However, in any case in which there is believed to be a serious risk that an unlawful killing by a third party will take place, Ministers must be consulted. The submission to Ministers will seek to address the relevant circumstances.

Rendition

9. Rendition was defined by the Intelligence and Security Committee in its 2007 report as any extra-judicial transfer of persons from one jurisdiction or State to another. While rendition may in some rare circumstances be lawful (and countries may differ in their interpretation of the relevant international law), it should be treated as unlawful detention for the purposes of this internal guidance. As such, in any case in which there is believed to be a serious risk that rendition will take place or has taken place, Ministers must be consulted.

Capital punishment

10. Capital punishment will be lawful in a number of countries with which the MOD is engaged, although it is contrary to UK Government policy. For the purposes of this internal guidance, it will be sufficient that, in any case in which there is believed to be a serious risk that someone will receive the death penalty, Ministers must be consulted (with the exception of the circumstances set out in para 19 where MOD will already have considered this risk when approving the detainee transfer route).